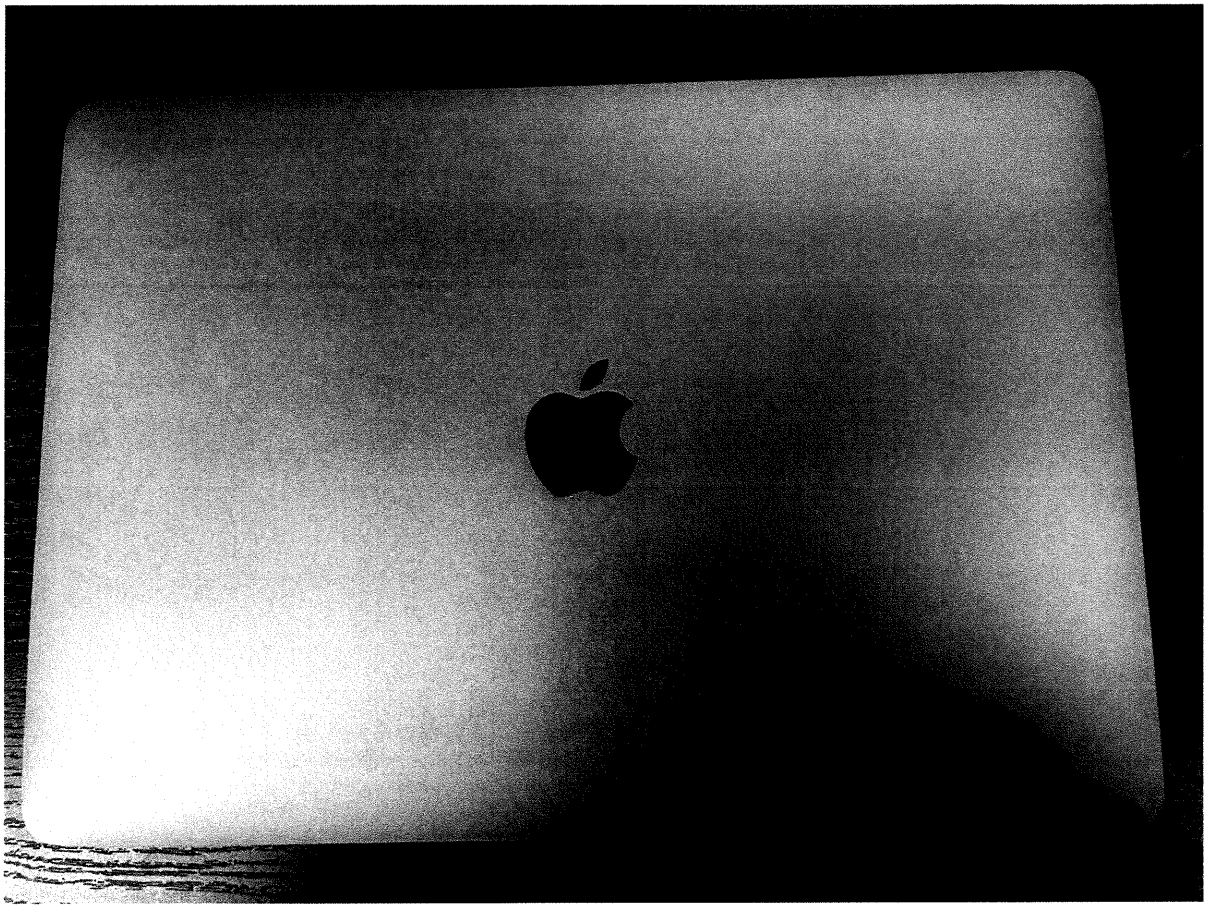
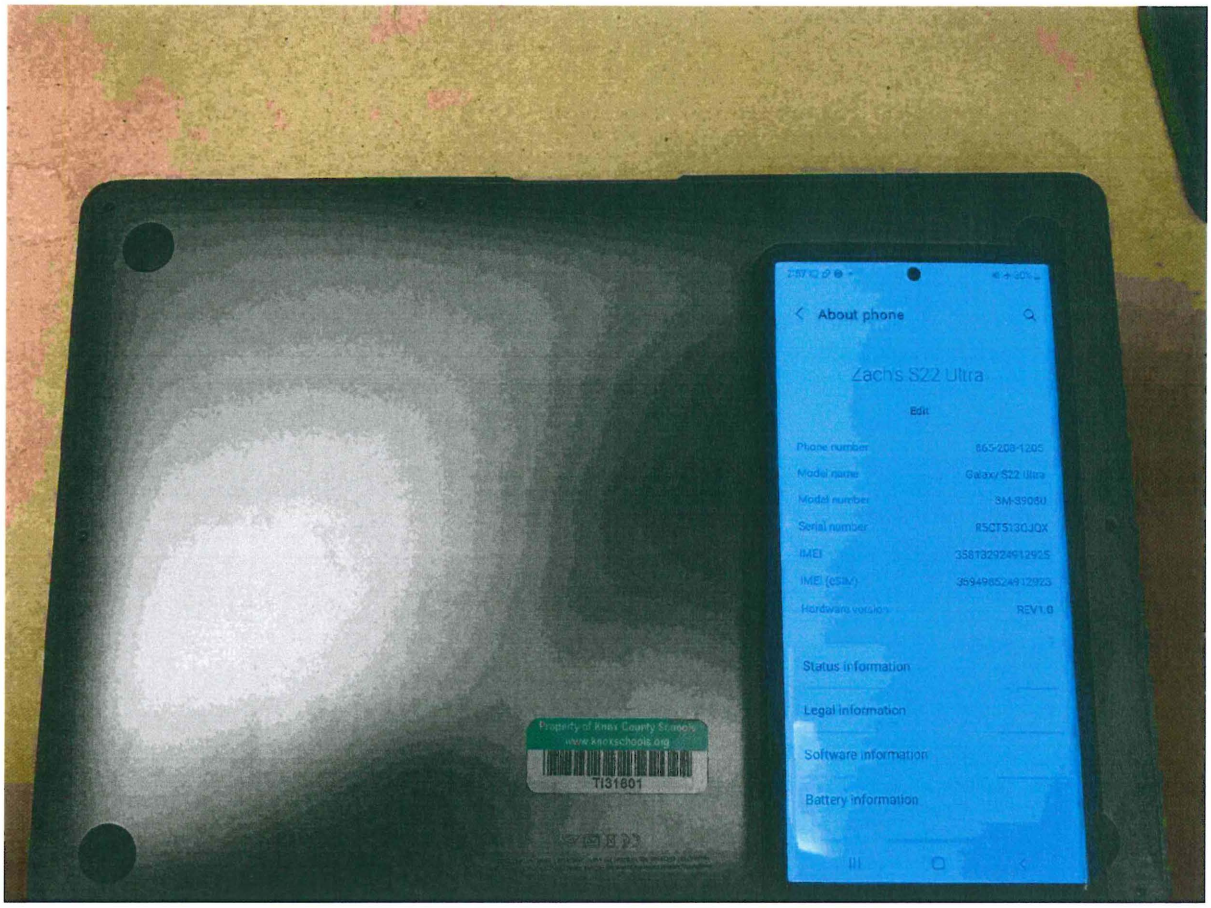
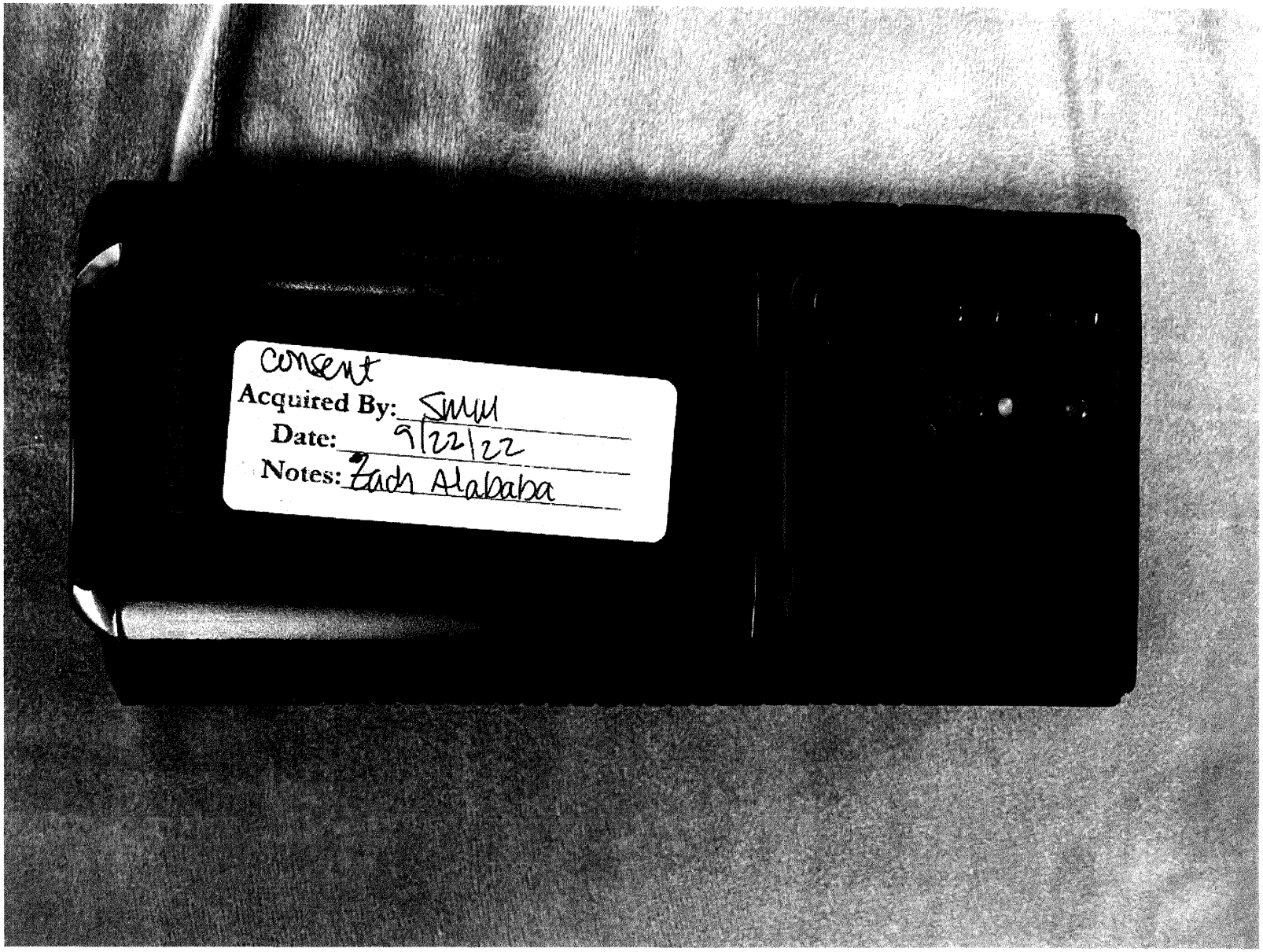
ATTACHMENT A

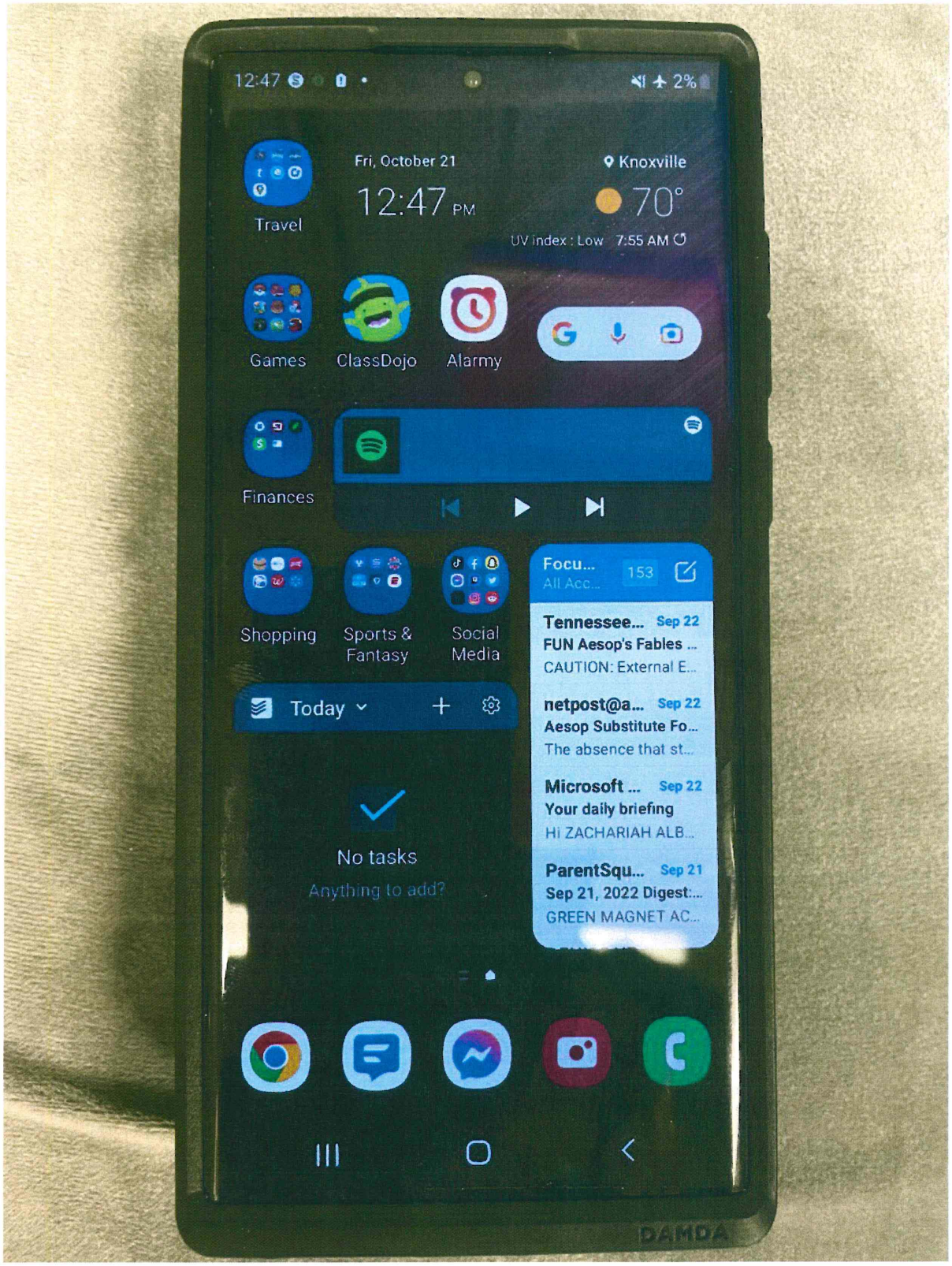
DESCRIPTION OF DEVICES TO BE SEARCHED

1. Silver Macbook Air laptop with Knox County School tag TI31801
2. Samsung Galaxy S22 Ultra Smartphone belonging to Zacharia Albaba




About phone
Zach's S22 Ultra
Edit
Phone number
Model name
Model number
Serial number
IMEI
IMEI (ESN)
Hardware version
Status information
Legal information
Software information
Battery information
Property of Knox County Schools
www.knoxschools.org
TI31601


Consent
Acquired By: SMM
Date: 9/22/22
Notes: Zach Alababa


12:47
2%
Travel
Fri, October 21
12:47 PM
Knoxville
70°
UV index : Low 7:55 AM
Games
ClassDojo
Alarmy
Finances
Shopping
Sports & Fantasy
Social Media
Today
No tasks
Anything to add?
Focu...
All Acc...
153
Tennessee... Sep 22
FUN Aesop's Fables ...
CAUTION: External E...
netpost@a... Sep 22
Aesop Substitute Fo...
The absence that st...
Microsoft ... Sep 22
Your daily briefing
Hi ZACHARIAH ALB...
ParentSqu... Sep 21
Sep 21, 2022 Digest:...
GREEN MAGNET AC...

ATTACHMENT B

Below is a list of items to be searched and seized from the devices described in ATTACHMENT A:

1. Images or visual depictions of child pornography;
2. Records and information containing child erotica, including texts, images and visual depictions of child erotica;
3. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to violations of the Subject Offenses;
4. Any and all information, notes, documents, records, or correspondence, in any format or medium, pertaining to child pornography or sexual activity with or sexual interest in minors;
5. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning Internet activity reflecting a sexual interest in minors or child pornography;
6. Any and all information, notes, software, documents, records, or correspondence, in any form and medium pertaining to any minor who is, or appears to be, the subject of any visual depiction of child pornography, child erotica, sexual activity with other minors, or that may be helpful in identifying any such minors;
7. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the Device or by other means for the purpose of committing violations of the Subject Offenses;
8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible child pornography;
9. Any and all information, records, documents, invoices and materials, in any format or medium, that concern any accounts with an Internet Service Provider pertaining to violations of the Subject Offenses;
10. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to violations of the Subject Offenses;
11. Records of Internet activity, including Internet Protocol addresses, firewall logs, transactions with Internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses pertaining to violations of the Subject Offenses or that show who used, owned, possessed, or controlled the Device;
12. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to use or ownership of the Device, or that aid in the identification of persons involved in violations of the Subject Offenses;
13. Credit card information, bills, and payment records pertaining to violations of the Subject Offenses;
14. Information about usernames or any online accounts or email addresses used to access or obtain images of child pornography;

15. Descriptions of time, date, locations, items, or events showing or tending to show the commission of, or connecting or tending to connect a person to violations of the Subject Offenses;

16. Evidence of who used, owned, or controlled the Device to commit or facilitate the commission of the crimes described, or at the time the things described in this warrant were created, edited, or deleted, including photographs, videos, logs, call logs, phonebooks, address books, contacts, IP addresses, registry entries, configuration files, saved usernames and passwords, documents, calendars, browsing history, search terms, metadata, user profiles, e-mail, e-mail contacts, messages (text or voice), instant messaging logs, file structure and correspondence;

17. Evidence of software that may allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security provisions or software designed to detect malicious software or unauthorized use of the device, and evidence of the lack of such malicious software;

18. Evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;

19. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;

20. Evidence of how and when the Device were used or accessed to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

21. The telephone number, ESN number, serial number, and/or SIM card numbers of or contained in the Device;

22. Passwords, encryption keys, and other access devices that may be necessary to access the Device; and

23. Contextual information necessary to understand the evidence described in this attachment.

DEFINITIONS

24. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

25. "Child Pornography" is defined in 18 U.S.C. § 2256(8), which includes as any visual depiction of sexually explicit conduct involving the use of a minor; a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaged in sexually explicit conduct; or a visual depiction that has been created, adapted, or modified to appear than an identifiable minor is engaging in sexually explicit conduct.

26. "Visual depiction" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

27. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not

necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

IN THE MATTER OF THE SEARCH OF: RESIDENTIAL PROPERTY LOCATED AT 139 CLEAR BRANCH ROAD, ROCKY TOP, TENNESSEE 37769	**Case No. 3:22-MJ-2178**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your affiant, Thomas Evans, an Investigator with the Knoxville Police Department (KPD) Internet Crimes against Children (ICAC) Task Force and being a Task Force Officer with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) being duly sworn, deposes and states the following:

1. Your affiant has been employed with the KPD since January 22, 1996. Your affiant has been assigned to the Knoxville Police Department's Internet Crimes Against Children Task Force (KPD-ICAC) as a computer examiner and undercover online investigator for the past twenty-two years. The KPD-ICAC Task Force is responsible for investigating and enforcing federal criminal statutes involving the sexual exploitation of children under Title 18, United States Code, Chapter 110, including, without limitation, section 2251(a), 2252A(a)(5)(B) and 2422(b).

2. Your affiant has acquired experience in these matters through specialized training and everyday work related to these types of investigations. Your affiant has completed the following training:

- 1996 Knoxville Police Department Training Academy Recruit Class A.

- 1997 Childhelp USA's Professional Training Conference.
- 1999 Protecting Children On-line provided by Fox Valley Technical College Criminal Justice Department, Appleton Wisconsin.
- 2000 Advanced Protecting Children On-line provided by Fox Valley Technical College, Criminal Justice Department.
- 2000 National Consortium of Justice Information and Statistics Training directed toward on-line investigation, tracking offenders and data recovery.
- 2000 40-hour course in the National White Collar Crime Data Recovery and Analysis.
- 2000 40-hour Internship with the Dallas Police Department's Internet Crimes Against Children Task Force.
- 40-hour internship with the Maryland State Police in October 2000 focusing on forensic software use in recovering computer-based evidence.
- 2001 Basic Class on EnCase computer forensic software.
- 2001 National Internet Crimes Against Children Training Conference in New Orleans focusing on the use of computer forensic utilities in evidence collection and Online Investigative Techniques.
- 2002 Crimes Against Children Conference in Dallas, TX focusing on online investigative techniques and computer forensic data recovery.
- 40-hour EnCase Intermediate Analysis and Reporting training in Sterling, VA April 2003.
- 2004 Silicon Valley ICAC Task Force Conference in San Jose, Ca with focus on online investigations and best computer forensic practices.
- 2004 Crimes Against Children Conference in Dallas, TX with emphasis on online investigative techniques and data recovery.
- December 2004 ICAC Investigative Techniques course in Knoxville, TN focusing on updated investigative techniques in online undercover operations.
- March 2005 EnCase Intermediate Analysis and Reporting course for computer examiners in Sterling, VA.
- May 2005 International Association of Computer Investigative Specialist 80-hour Forensic Computer Examiner Training Program in Orlando, FL.

- Recognized in April 2005 by the International Association of Computer Investigative Specialists as a Certified Electronic Evidence Collection Specialist.

- 2005 National ICAC Conference in Dallas, TX focusing on characteristics of the Internet offender and online undercover operations.

- Knoxville Police Department Basic Investigator Class January 30- February 3, 2006.

- 2006 National Crimes Against Children Conference in Dallas, TX focusing on online undercover Investigative Techniques.

- December 2006 FTK Boot camp held at Pellissippi State Technical College for computer forensic training using the Access Data Ultimate Toolkit software package.

- January 2007 Internet Crimes Against Children Task Force Operation Peer Precision Training in Tallahassee FL focusing on online undercover Peer-to-Peer investigations.

- June 12, 2008 F.B.I. CART ImageScan training concentrating on the use of the ImageScan System for secure computer previews and data recovery.

- April 11- May 14th 2010 United States Secret Service BCERT Computer Forensic training Hoover, AL.

- January 2011 assigned to the United States Secret Service Electronic Crimes Task Force for East Tennessee.

- February 21-23rd 2012 Tennessee ICAC Training conference in Nashville, TN focusing on cell phone investigations, human trafficking, undercover P2P investigations (instructed), and open source computer forensic tools.

- USDOJ 2012 National Law Enforcement Training Conference in Atlanta GA April 17-19th, 2012 focusing on P2P undercover investigations, Craigslist undercover investigations, Gigatribe investigations, and the psychological profile of a child pornography collector.

- June 13-17th Internship with the Citrus County Sheriff's Department regarding E Commerce undercover investigations (Operation Summer Nights).

- February 5th - 8th 2013 ICAC eMule P2P investigations.

- March 26-28th 2013– Tennessee ICAC state conference in Nashville, TN focusing on Commercial Sexual Exploitation of Children (CSEC).

- October 28-31, 2013 Tennessee ICAC state conference in Nashville, Tennessee, focusing on forensic preview tools, ICAC legal updates and virtual machine utilization for computer forensics and undercover investigations.

- February 24-26, 2014 – Tennessee ICAC state conference in Nashville, TN, focusing on computer previews, Google Security, and locating wireless devices.

- April 15-17, 2014 – 2014 Regional ICAC Law Enforcement Training on Child Exploitation focusing in court testimony, Ares Peer to Peer investigations, National Center for Missing and Exploited Children Law Enforcement Portal, and characteristics of the offender.

- September 18-19, 2014 – Westminster, Colorado ICAC BitTorrent Investigations.

- April 20-22, 2015 – Brentwood, Tennessee – Tennessee ICAC state conference focusing on online undercover chat investigations, legal updates, and human sex trafficking.

- November 11-13, 2015 – Gatlinburg, Tennessee – Tennessee ICAC conference focusing on current chat trends, P2P file sharing investigations, and on scene preview techniques and software.

- March 28-30, 2016 – Nashville, Tennessee – Tennessee ICAC conference focusing on legal updates, use of polygraph in conjunction with child pornography cases and online undercover operations.

- April 18, 2016 – Atlanta, Georgia – National ICAC Conference focusing on online undercover investigations, interviewing offenders, legal updates, psychology of the internet offender and on scene computer forensic tools.

- May 2, 2016 – Knoxville, Tennessee – Federal Bureau of Investigation Legal Training.

- October 17-19, 2016 – Chattanooga, Tennessee – Tennessee ICAC State Conference focusing on Legal Updates, Anonymity and Darknet, and IP Version 6.

- February 27- February 28, 2017 – Atlanta, Georgia – Darknet Training. Training focused on anonymous Darknet applications for the trafficking of child pornography.

3. As a federal task force officer, your affiant is authorized to investigate violations of the laws of the United States and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

4. This affidavit is made in support of an application for a warrant to search the premises located at 139 Clear Branch Rd., Rocky Top, TN 37769. This residence is more particularly described in ATTACHMENT A, a copy of which is attached hereto and incorporated by reference herein.

5. Information contained within the affidavit is based upon information I have gained from my investigation, my personal observations, my training and experience, and/or information related to me by other law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning the investigation. I have set forth only the facts which I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, and 2422(b) described in ATTACHMENT B, are presently located at the premises described in ATTACHMENT A.

GLOSSARY OF TERMS APPLICABLE TO THIS AFFIDAVIT

6. INTERNET SERVICE PROVIDER (ISP): A company that provides its customers with access to the Internet, usually over telephone lines or cable connections. Typically, the customer pays a monthly fee, and the ISP supplies software and/or hardware that enables the customer to connect to the Internet by a modem or similar device attached to or installed in a computer.

7. THE INTERNET: The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across county, state, and national boundaries.

8. INTERNET PROTOCOL ADDRESS (IP Address): The unique numeric address of a machine or computer attached to and using the Internet. This address is displayed in four blocks of numbers, e.g., 123.456.789.001. One computer or device can only use each numbered IP address over the Internet at a time.

9. WHISPER: Whisper is a free-access anonymous social media application and online platform where users engage in conversations without identities or profiles.

10. ACCURINT: Accurint is a widely used and accepted as a tool to locate and research publicly available records. Accurint is used by government, commercial, and law enforcement agencies to obtain publicly available information and has been utilized by myself numerous times in previous investigations. Accurint has proved reliable in each previous investigation.

COMPUTERS AND CHILD PORNOGRAPHY

11. Your affiant has received extensive online undercover training as well as computer forensics training in reference to computer related criminal investigations. Your affiant knows all of the below-described information as the result of his training and experience in the investigation of computer-related crime and by conferring with other law enforcement personnel who investigate computer-related crime.

12. Your affiant knows that, computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It also has revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant

resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

13. The advancement in technology of computers, smartphones and tablets has added to the methods used by child pornography collectors to interact with and sexually exploit children. Each of the above serves six functions in connection with child pornography. These are production, communication, distribution, receipt, advertisement and storage.

14. Child pornographers can now produce both still and moving images directly from a common video camera, small action style cameras such as a GoPro, smartphones, laptop computers equipped with web cameras, and tablets. In the past, a camera could be attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred, or printed directly from the computer, external hard drive, media card (SD, Compact Flash, micro SD, memory stick), smart phone, tablet, iPod or iPad. The captured image can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is inexpensive and technically easy to produce, store, and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow, as had been the case in the past. Your affiant has been involved in recent investigations where digital cameras, smart phones, tablets, and webcams were used to produce child

pornography and store said child pornography either on the device, personal computer or removable media of the subject.

15. New technology now allows child pornographers to use even smaller digital devices like smartphones and tablets that have digital cameras and video recording capability built directly into the devices. These devices are equipped with their own processors and memory that allow the devices to actually perform as small mini computers. With the use of free and publicly available apps, a child pornographer has the ability to produce child pornography, receive and distribute it in a matter of just a few seconds and maintain relative anonymity using free open wireless access points.

16. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer has changed that. A device known as a modem allows any computer to connect to another computer through the use of telephone and/or cable lines. By connecting to a host computer, electronic contact can be made with literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. These host computers are sometimes operated by commercial concerns, such as Bellsouth, AT&T and America Online, which allow subscribers to dial a local number and connect to a network which is in turn connected to their host systems. Today many ISPs, such as Comcast Communications and Charter Communications, offer high-speed broadband Internet service. Broadband is often called high-speed Internet because it usually has a high rate of data transmission much higher than the dial-up or DSL structure of the past. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web. Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of "chat rooms" and/or instant messaging.

17. These communication structures are ideal for individuals who possess, receive and distribute child pornography. They provide open and anonymous communication, allowing users to locate other persons who share their interest in child pornography, while maintaining their anonymity. Once contact has been established, it is then possible to send text messages, graphic images, and high-resolution video to other individuals interested in child pornography. Moreover, the child pornographer need not use the large service providers. Child pornographers can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornographers.

18. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred via electronic mail to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services, P2P services and easy access to the Internet, computers, tablets, and smartphones are a preferred method of receipt and distribution of child pornographic materials.

19. The computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly consisting of hard drives) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two terabytes are not uncommon. The KPD-ICAC computer examiners routinely examine computer hard drives of 1 Terabyte (1000 gigabytes) and more in

child pornography cases. These drives can store hundreds of thousands of images and video at very high resolution and quality. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, save the image, and store it at another location. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful examination of electronic storage devices is it possible to recreate the evidence trail.

20. Based on your affiant's knowledge, training and experience and training and experience of other officers, your affiant knows that child pornographers commonly download and save some of their collection of child pornography from their computer to removable media such as thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, smart televisions, computer game consoles (Sony PlayStation, Xbox), tablets, iPods or iPads so the images can be maintained in a manner that is both mobile and easily accessible to the collector. It is not uncommon for the child pornographer to print pictures of child pornography and to keep them in a safe and secure location for easy viewing. Thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, smart televisions, computer game consoles (Sony PlayStation, Xbox), tablets, iPod's or iPads, containing child pornography and printed pictures of child pornography are not only kept near the computer, but also in hidden areas known to the child pornographer, to keep other individuals from discovering the illegal material. For example, a search warrant executed by other officers known to your affiant resulted in the finding of a hard drive wrapped in plastic hidden under a bathroom sink. Additionally, your affiant knows that in 2014, investigators with the KPD-ICAC Task Force arrested a subject for the interstate travel to meet a minor for sexual purposes (18 U.S.C. § 2423(a)). An external hard drive was located in the trunk of the suspect vehicle. A search warrant on the external hard drive revealed a contact

offense by the subject on a four-year-old girl and numerous pornographic videos of the sexual abuse produced by the subject utilizing his smartphone.

21. Your affiant states that computer technology can be mobile in the form of laptop computers, removable thumb drives, removable hard drives, media cards (SD, Compact Flash, micro SD, memory stick), computer game consoles (Sony PlayStation, Microsoft Xbox), smart phones, iPad's, iPod's, tablets, or accessible via remote or wireless means. Therefore, evidence, contraband, instrumentalities, or fruits of crime can be located virtually anywhere within the residence or vehicle of a child pornographer. Your affiant has been involved in child pornography investigations where child pornography was found on removable media located in a suspect's vehicle. Your affiant has also been involved in investigations where smartphone (Android) emulators were utilized on a computer to allow the user to use applications that had been installed and utilized on the subject's smartphone. Additionally, child pornography can remain on devices indefinitely unless the user takes active steps to delete or overwrite the digital files of child pornography. For example, your affiant is aware of a recent Knoxville Police ICAC P2P file sharing investigation with child pornography dating back to 2009. Additionally, recent investigations have revealed that some P2P suspects in order to remain safer have instituted the methodology of downloading child pornography then deleting it after a short period of time. Based on information I have gained from interviews with child pornographers that utilized the above described method, the suspects indicated they felt an increased level of security knowing the child pornography was not stored on the computer/devices for long periods of time and that they could re-download mass amounts of child pornography at any time. However, computer exams have revealed that even if the above methodology is utilized examiners are able to locate and recover evidence about the criminal activity including but not limited to the files child pornography, software used to locate and download child pornography,

log files identifying specific child pornography files that have been downloaded and chat/messaging conversations that have occurred through use of the suspect computer system.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

22. Based on your affiant's training and experience, your affiant knows that the search of computers and retrieval of data from computer systems and related media, often requires agents to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a) Computer storage devices like thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, smart televisions, computer gaming consoles (Sony PlayStation, Xbox), tablets, iPods or iPads can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b) Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is

extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from a destructive code imbedded in the system such as a "booby trap," a controlled environment is essential to its complete and accurate analysis.

23. Based upon your affiant's training and experience and consultation with experts in computer searches, data retrieval from computers, and related media, as well as consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, your affiant knows that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all computer system input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the systems data in a laboratory or other controlled environment. This is true because of the following:

a) The peripheral devices, which allow users to enter or retrieve data from the storage devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, and/or data security devices are not necessary to retrieve and preserve the data after inspection, the government will return the material in a reasonable time.

b) In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as the central processing unit. Further, the analyst

needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

c) The Knoxville Police Department's ICAC Task Force, currently conducts onsite previews of computers in order to focus and seize only devices containing contraband. This process assists investigators with only seizing and examining items associated with the criminal activity. Based on experience, cooperation from occupants of the residence being searched assists investigators with identifying and seizing only devices that will contain contraband. It is important to note that systems currently powered off will not be powered on to conduct a preview unless investigators believe turning on the device will not alter or destroy possible evidence.

24. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime of advertising, distribution, receipt, and/or possession of child pornography in violation of the law and should all be seized as such.

25. Based on your affiant's training and experience in computer searches and data retrieval from computers while in a laboratory setting, your affiant is aware that such searches can be complex and time consuming.

PROBABLE CAUSE

26. On August 15, 2022, your affiant received information from Investigator Matt Hedden with the Kentucky Office of the Attorney General / Department of Criminal Investigations. Investigator Hedden is the Special Victims Unit Director and also a United States Secret Service (USSS) Task Force Officer assigned to work Internet Crimes Against Children (ICAC) cases with the Kentucky Office of the Attorney General.

27. During an authorized undercover operation, Investigator Hedden posing as a minor female posted an online "ad" on the social media application known as "Whisper". The ad posted by Inv. Hedden contained a background image of a fully clothed undercover female persona with the words "Start a new school in a few days. Kinda Nervous". This advertisement was active on August 10, 2022.

28. On August 10, 2022 an individual known only as "Hey!" on the Whisper application began messaging the undercover persona. During the conversation the subject known only as "Hey!" initiated sexual communication as well as solicited sexually explicit images of the undercover minor persona.

29. Below are exerts from the conversation between "Hey!" and the undercover persona identifying themselves as "Katie" on the Whisper application.

> From Hey! : I'd love to get to know you. You look so so beautiful! Also, I used to live in Kentucky! I'm 31. Hbu beautiful? I'm a teaqcher too and yeah I miss Kentucky....I'm an elementary PE teacher. How old are you?
>
> From Katie: Ur gonna b mad 14...Idc that ur older
>
> From Hey!: Ok bc tbh I don't care that you're younger.....are you interested in getting to know each other better? You wanting a bf or fwb or daddy or something?
>
> From Katie: Yeah maybe How far re from Ashland
>
> From Hey!: I live in Knoxville...I'm about 2 hours from Ashland. Defintely drivable!
>
> From Hey!: I'd love to make you my girlfriend I'd love that ! What's y our name?
>
> From Katie: Katie What's urs
>
> From Hey!: Zach!
>
> From Hey!: Lol I find you very very attractive and it's gonna be hard to behave sometimes but I will for you....Tbh seeing those pictures of you has made me want you really badly....I loveeeeee freckles and braces tbh haha...if we kissed, idk if I would be able to stop....:ole O'm really turned on and wanting you rn. You made me hard....Also, can I ask you something babe, and you can say no if it makes you uncomfortable. Can I see more your beautiful body? I'm hard and I want to cum for you.

From Hey!: Babe, I'm about to finish. Can I see a naughty pic or two of you your're comfortable? I really want you to be my gf. I'm crazy about you already....I'd love to be your boyfriend, beautiful.

From Katie: "Idw b preggers" (meaning I don't want to be pregnant)

From Hey!: We will use a condom babe. I won't get you preggers lol.....I promise I won't! We will use comdoms and I won't be inside you when I cum....What if I kissed your chest and sucked your boobs and after I did that I kissed down your stomach and used my mouth on you?

30. Investigators issued a search warrant to Whisper for account information pertaining to the user Hey! to include IP addresses used for accessing the Whisper social media site. Whisper responded with an IP address of 71.203.231.65 to be associated with the Hey! Whisper user account. The IP address of 71.203.231.65 was determined to belong to Comcast Communications and geolocates to Rocky Top, Tennessee. Your affiant knows that Lake City, Tennessee recently changed its name to Rocky Top, Tennessee in 2014.

31. A subpoena for subscriber records was issued to Comcast for the above IP address of 71.203.231.65 on 08-31-2022 at 18:22 UTC. Comcast returned the following information pertaining to the subscriber of the IP address of 71.203.231.65:

Subscriber Name:	Zach Albaba
Service Address:	139 Clear Branch Rd. Lake City, TN 37769
Billing Address:	139 Clear Branch Rd Lake City, TN 37769
Telephone #:	865-208-1205
Type of Service:	Internet
Account Number:	8396500200038242
Account Status:	Active
IP Assignment:	Dynamically Assigned

Current IP: 71.203.231.65

Email User Id: zachalbaba@comcast.

32. During the undercover communication, images received from the Whisper user known as Hey! depicted a white male appearing to be in his thirties with dark hair. Open source investigation revealed that Zach Albaba was currently employed as a PE teacher at Green Magnet Academy located at 801 Lula Powell Drive, Knoxville, TN 37915. Investigators reviewed the Green Magnet Academy website and identified the image posted of PE teacher Zach Albaba to be the same person in the images sent by the Whisper user Hey! to the undercover account of Katie.

33. Your affiant searched the Tennessee Criminal Justice Portal and found a Tennessee Driver license issued to Zachariah Luaie Albaba, D.O.B. 04/09/1991 with address of 143 Clear Branch Rd., Lake City, TN 37769. (Note: This address appears to the be the address of his parents Charlie and Elizabeth Pickrell based on information from the United States Postal Service.) A Toyota 4 door sedan with license plate 8A69T0 is registered to Zacharia L Albaba at 139 Clear Branch Rd., Rocky Top, TN 37769.

34. On or about 09/19/2022, your affiant as well as USSS agents conducted surveillance at Green Magnet Academy located at 801 Lula Powell Drive, Knoxville, TN 37915. A silver Toyota Corolla 4 door with Anderson County Tennessee tag of 8A6-9T0 registered to Zacharia L. Albaba was located parked in the staff parking lot of the school. The vehicle had a "University of Kentucky" window sticker in the lower portion of the rear window.

35. Your affiant conducted open-source research and determined that Zach Albaba is married to Ashley Noelle Albaba formerly Ashley Gregg. A check of the Tennessee Criminal Justice Portal showed that Ashley Albaba D.O.B. 09/29/1990 resides at 139 Clear Branch Rd., Lake City, TN 37769. Additionally, surveillance on 09/19/2022 at 139 Clear Branch Rd., Rocky

Top, TN identified a dark colored Kia sedan with TN license plate BHV8252 registered to Ashley Gregg who resides at 139 Clear Branch Rd., Rocky Top, TN 37769.

36. Your affiant also personally viewed the images sent to the undercover account from the Whisper user Hey! and compared them to the Tennessee driver license photo and Green Magnet School website photo and confirmed all of the images were of Zacharia L. Albaba.

37. Your affiant performed a law enforcement check using Accurint for the phone number of 865-208-1205. Accurint is used by government, commercial, and law enforcement agencies to obtain publicly available information and has been used by your affiant in numerous times in previous investigations over the years. The Accurint check of the phone number 865-208-1205 shows the number belonging to Zacharia L. Albaba residing at 139 Clear Branch Rd. Rocky Top, Tennessee 37769.

38. On 09/20/2022, your affiant conducted surveillance of 139 Clear Branch Rd., Rocky Top, TN 37769. Your affiant observed two vehicles parked directly behind the residence. A dark colored Kia sedan corresponding to Ashley Albaba and a silver Toyota Corolla corresponding to Zacharia Albaba were observed in the driveway behind the first trailer (gray in color) located at 139 Clear Branch Rd., Rocky Top, TN 37769.

CONCLUSION

39. Based on the aforementioned information, your affiant respectfully submits that there is probable cause to believe that a computer and/or electronic devices located at 139 Clear Branch Rd., Rocky Top, TN 37769, are being used for the purpose of online enticement of minors for sexual purposes. Your affiant bases this belief on the fact that on or about August 10, 2022, an undercover officer posing as a 14-year-old minor female (Katie) in the Ashland Kentucky area on the social media platform known as Whisper was contacted by Zacharia Albaba (Hey!) for the purpose of enticing the minor female into sexual conduct. Zacharia

Albaba, knowingly used a facility or means of interstate commerce, to persuade, induce and entice the undercover officer posing as a 14-year-old female to entice the minor in sexual activity.

40. Additionally, your affiant knows that Zacharia Albaba is currently employed at Green Magnet Academy in Knoxville Tennessee as a PE teacher. Zacharia Albaba's name and picture are on the Green Magnet Academy website in the staff directory. Your affiant compared the images sent by the Whisper user (Hey!) to the Green Magnet School website staff directory and the Tennessee Criminal Justice Portal driver license picture of Zacharia Albaba and observed them to be of the same person. Your affiant conducted surveillance at Green Magnet Academy and observed a gray Toyota Corolla Tennessee license plate 8A6-9T0 in the staff parking lot. The vehicle is registered to Zacharia Albaba residing at 139 Clear Branch Rd., Rocky Top, Tennessee 37769.

41. Further, there is probable cause to believe that evidence, fruits, and instrumentalities of this crime, which are listed specifically in Attachment B, which is incorporated herein by reference, are presently located on the premises described in Attachment A. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time and to examine, analyze and test them.

42. The evidence, fruits and instrumentalities of violation of Title 18, United States Code, Section 2422(b), believed to be concealed at the premises described in Attachment A, are listed in Attachment B of this affidavit, which is incorporated herein.

43. Therefore, your affiant respectfully requests issuance of a search warrant authorizing the search and seizure of the items listed in Attachment B.

Tom Evans
Investigator
Knoxville Police Department
Internet Crimes Against Children Task Force

Sworn and subscribed before me

This 21st day of September 2022.

HONORABLE JILL E. MCCOOK
UNITED STATES MAGISTRATE JUDGE